

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN**

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 15-CR-163

PHILLIP A. EPICH,

Defendant.

RECOMMENDATION ON DEFENDANT'S MOTION TO SUPPRESS

On August 11, 2015, a grand jury sitting in the Eastern District of Wisconsin returned a two-count indictment against the defendant, Phillip A. Epich.

(Indictment, ECF No. 18.) Count One charges Mr. Epich with knowingly receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and Count Two charges Mr. Epich with knowingly possessing matter that contained images of child pornography, in violation 18 U.S.C. § 2252A(a)(5)(B). On August 19, 2015, Mr. Epich pled not guilty to both counts charged in the Indictment. (Minute entry for arraignment and plea hearing, ECF No. 24.) The matter is assigned to United States District Judge Rudolph T. Randa for trial and to this Court for pretrial motions. Trial in this matter is adjourned.

Currently pending before this Court is Mr. Epich's motion to suppress, which he filed on September 24, 2015. For the reasons that follow, the Court will recommend that Mr. Epich's motion to suppress be denied.

I. Investigative Background

In September 2014, agents from the Federal Bureau of Investigation began investigating a website that appeared to be dedicated to the advertisement and distribution of child pornography. The website operated on the anonymous Tor network, which allowed users to mask their Internet Protocol addresses while accessing the website. In February 2015, the FBI apprehended the website's administrator and assumed administrative control of the site. The FBI allowed the site to continue to operate from a computer server that was located at a government facility in Newington, Virginia.

On February 20, 2015, a United States Magistrate Judge in the Eastern District of Virginia issued a warrant authorizing the government to deploy a network investigative technique (NIT) on the computer server running the seized website. (NIT Warrant and Application, ECF No. 41-1.) Essentially, the NIT allowed the government to obtain the true IP address of computers that logged onto the website. The government deployed the NIT from February 20, 2015, until March 4, 2015.

During the investigation, law enforcement agents identified "Redrobin16" as a user of the website. Agents obtained Redrobin16's IP address using the NIT, and subsequent investigation linked this IP address to Mr. Epich at his home in West Allis, Wisconsin. On July 16, 2015, United States Magistrate Judge William E. Duffin issued a warrant authorizing the search of Mr. Epich's residence. (Residence Warrant and Application, ECF No. 41-2.) Agents executed the warrant the following

day and recovered, among other things, a desktop computer that contained evidence of searching for and viewing child pornography. Mr. Epich was then arrested pursuant to a criminal complaint that charged him with receiving child pornography.

Agents subsequently seized a thumb drive that was kept in Mr. Epich's home but not found during the initial search. On August 6, 2015, United States Magistrate Judge Nancy Joseph issued a warrant authorizing the search of the thumb drive. (Thumb Drive Warrant and Application, ECF No. 41-3.) The thumb drive contained additional child pornography.

II. Discussion

Mr. Epich seeks an order suppressing all evidence and derivative evidence obtained as a result of the searches of his home and property. (Motion to Suppress, ECF No. 34.) As grounds for his motion, Mr. Epich argues that the warrants to search his residence and thumb drive are invalid because they relied extensively on the "deeply flawed" NIT Warrant. (*Id.* at 1.) More precisely, he maintains that the government would not have been able to secure the Residence Warrant or the Thumb Drive Warrant without information—namely, his IP address—derived from the NIT Warrant. He further asserts that an evidentiary hearing is not necessary because his argument is limited to the four corners of the search warrant affidavits. (*Id.* at 1.) Thus, the Court will begin by summarizing the contents of those documents.

A. Search warrants and supporting documents

On February 20, 2015, an FBI Special Agent applied for a warrant to use an NIT to investigate the users and administrators of a website that was believed to be dedicated to child pornography. In support of the warrant application, the agent submitted a thirty-three-page affidavit that set forth his basis for probable cause to believe that deploying the NIT would uncover evidence and instrumentalities of certain child exploitation crimes. (Affidavit in support of application for NIT Warrant [hereinafter NIT Warrant Affidavit], ECF No. 41-1 at 6-38.)

After describing background information concerning federal investigations related to child pornography and the sexual exploitation of children, (*id.* ¶¶ 1-5), the affidavit discusses the anonymous nature of the target website. The website operated on the anonymous Tor network, which users could access only after downloading specific Tor software. (*Id.* ¶ 7.) Use of “[t]he Tor software protect[ed] users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address.” (*Id.* ¶ 8.) Thus, the Tor network neutralized traditional methods utilized to identify users who visited particular websites. The Tor network also allowed users to host entire websites as “hidden services,” which prevented law enforcement agents and other users from determining the location of the host computer. (*Id.* ¶ 9.)

The affidavit then discusses how users could find and access the website. Because the website was set up as a hidden service, it did not reside on the

traditional Internet. (*Id.* ¶ 10.) Rather, a user could access the site only through the Tor network and only if the user knew the site's exact web address. A user could learn the web address from other users of the site or from other Internet postings describing the site's content and location. Given the "numerous affirmative steps" required to access the website, the affidavit states that it would be "extremely unlikely that any user could simply stumble upon [the site] without understanding its purpose and content." (*Id.*) Further, the main page of the site contained "images of prepubescent females partially clothed and whose legs are spread." (*Id.*) The affidavit thus concludes that any user who successfully accessed the website had knowingly done so with intent to view child pornography. (*Id.*)

Next, the affidavit describes the nature and content of the website. The site "appeared to be a message board website whose primary purpose [was] the advertisement and distribution of child pornography." (*Id.* ¶ 11.) The first post was made in August 2014 and, at the time the affidavit was submitted, the website contained 95,148 posts, 9,333 total topics, and 158,094 members. The main page of the site contained "two images depicting partially clothed prepubescent females with their legs spread apart." (*Id.* ¶ 12.) Text underneath the images read, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." (*Id.*) The affiant explained that, based on his training and experience, "no cross-board reports" referred to "a prohibition against material that is posted on other websites from being 're-posted' to [the website]," and ".7z" referred to "a preferred method of compressing large files or sets of files for distribution." (*Id.*)

Before logging onto the website, users had to register an account by accepting the site's registration terms and entering a username, password, and email address. (*Id.* ¶¶ 12-14.) The registration terms advised users to provide a fake email address and emphasized the anonymous nature of the site. (*Id.* ¶ 13.) The entire text of the registration terms was included in the affidavit. (*See id.*)

Upon registering and logging on, users could observe all the of sections, forums, and sub-forums contained on the website, along with the corresponding number of topics and posts in each category. (*Id.* ¶¶ 14-19.) Many of the sections were subdivided by age (e.g., "Jailbait" or "Pre-teen"), gender (boys or girls), and/or level of explicit conduct (hardcore or softcore). Several of the forums "contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users." (*Id.* ¶ 17.) The remaining forums contained "numerous images that appeared to depict child pornography . . . and child erotica," and the affidavit describes, in graphic detail, several examples of images depicting prepubescent females being sexually abused by adult males. (*Id.* ¶ 18.) The website also contained a private messaging feature, which the affiant believed was used "to communicate regarding the dissemination of child pornography," as well as other features that were used to facilitate the advertisement, distribution, and sharing of child pornography. (*Id.* ¶¶ 20-25.)

After describing the identification and seizure of the website's administrator and host computer server, (*id.* ¶¶ 28-30), the affidavit details the NIT and how it would be deployed on the site. Given the anonymity provided by the Tor network,

traditional investigative procedures had failed or were unlikely to uncover the identities of the site's administrators and users. (*Id.* ¶ 31.) According to the affiant, however, the NIT had "a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location of those users and administrators of [the site]" who were violating federal laws concerning child pornography and the sexual exploitation of children. (*Id.*)

The NIT would be deployed each time a user logged onto the website while it was running on a computer server located at a government facility in the Eastern District of Virginia. (*Id.* ¶ 36.) The NIT involved additional computer instructions that would be downloaded to a user's computer along with the site's normal content. (*Id.* ¶ 33.) After downloading the additional instructions, the user's computer would transmit certain information to a government-controlled computer that was located in the Eastern District of Virginia, including: (1) the computer's actual IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's "Host Name"; (6) the computer's active operating system username; and (7) the computer's "Media Access Control" address. (*Id.* ¶¶ 33-34, 36.)

The affidavit describes how each category of information "may constitute evidence of the crimes under investigation, including information that may help to identify the . . . computer and its user." (*Id.* ¶ 35.) As just one example, the computer's actual IP address could be associated with an Internet Service Provider

and a particular ISP customer. The affidavit requested authorization to use the NIT for thirty days. (*Id.* ¶ 36.)

A United States Magistrate Judge in the Eastern District of Virginia signed the NIT Warrant on February 20, 2015. (NIT Warrant, ECF No. 41-1 at 3-5.) Agents executed the warrant that same day and continued to collect data from computers that accessed the website until March 4, 2015. (NIT Warrant Return, ECF No. 41-1 at 39-40.)

On July 16, 2015, an FBI Special Agent applied for a warrant to search a residence located in West Allis, Wisconsin. In support of the warrant application, the agent submitted a thirty-one-page affidavit that set forth his basis for probable cause to believe that the residence contained evidence relating to federal violations concerning child pornography. (Affidavit in support of application for Residence Warrant, ECF No. 41-2 at 10-40.)

After discussing the affiant's training and experience, the relevant statutes, and definitions of terms used therein, (*id.* ¶¶ 1-29), the affidavit describes the investigative background and the specific facts establishing probable cause. The affidavit indicates that Mr. Epich "[had] been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network." (*Id.* ¶ 30.) Reciting much of the information contained in the NIT Warrant Affidavit, the affidavit then describes the nature of the Tor network, the content of the website, and the government's use of the NIT. (*Id.* ¶¶ 31-48.)

Next, the affidavit explains how law enforcement agents identified Mr. Epich as a suspected user of the website. An individual with the username “Redrobin16” registered an account on the website on February 19, 2015, and accessed the site several times between February 19 and February 24, 2015. (*Id.* ¶¶ 49-54.) This user accessed several posts that contained links to and sample photos of child pornography. Agents learned the user’s IP address via the NIT, determined the service provider of the IP address, and linked the IP address to Mr. Epich at his residence in West Allis. (*Id.* ¶¶ 50-60.)

Judge Duffin signed the Residence Warrant on July 16, 2015, (Residence Warrant, ECF No. 41-2 at 1-8), and law enforcement agents executed it the following day, (Affidavit in support of application for Thumb Drive Warrant [hereinafter Thumb Drive Warrant Affidavit], ECF No. 41-3 at 6-13). During the search of Mr. Epich’s residence, agents recovered a desktop computer that contained evidence of searching for and viewing child pornography. (Thumb Drive Warrant Affidavit ¶ 5.) Mr. Epich was then arrested and charged in federal court with receiving child pornography. (*Id.* ¶ 6.) Subsequent investigation led agents to seize a thumb drive that Mr. Epich kept in his residence but which was not found during the initial search. (*Id.* ¶¶ 7-9.)

On August 6, 2015, an FBI Special Agent applied for a warrant to search the thumb drive. In support of the warrant application, the agent submitted an eight-page affidavit that set forth his basis for probable cause to believe that the thumb drive contained evidence relating to federal violations concerning child

pornography. The affidavit indicates that agents interviewed Mr. Epich and that he admitted to using his desktop computer to view child pornography. (*Id.* ¶ 6.) To establish probable cause, the affiant also attached a copy of the Residence Warrant and its supporting application and affidavit. (*See* ECF No. 41-3 at 14-53.)

Judge Joseph signed the Thumb Drive Warrant on August 6, 2015. (Thumb Drive Warrant, ECF No. 41-3 at 1-4.) Forensic analysis revealed that the thumb drive contained child pornography.

B. Analysis

According to Mr. Epich, the NIT Warrant “was unique in scope and breadth.” (Mot. at 2.) More precisely, he argues that the warrant is deeply flawed because it “failed to establish probable cause, failed to meet the Fourth Amendment’s particularity requirements, failed to show that the searches would recover evidence of a crime, and violated the Federal Rules of Criminal Procedure.” (*Id.*) The Court will address each argument in turn.

1. The warrant’s compliance with the Fourth Amendment

Mr. Epich first argues that the NIT Warrant failed to comport with the requirements of the Fourth Amendment. (*Id.* at 10-22.) Specifically, he maintains that the affidavit submitted in support of the NIT Warrant

failed to establish probable cause because it applied to any person who logged onto the website even though: (1) the website did not warn potential users that it contained illegal materials; (2) users can visit and use the website without looking at any illegal material; [and] (3) the warrant could have, but failed, to differentiate between different users.

(*Id.* at 10-19.) Thus, according to Mr. Epich, the NIT Warrant Affidavit failed to establish probable cause to believe that *every person* who logged onto the website committed a crime. (*Id.* at 19; Reply in Support of Motion to Suppress, ECF No. 47 at 2; Response to Government’s Sur-reply, ECF No. 52 at 1.) He further maintains that the affidavit failed to meet the Fourth Amendment’s particularity requirement because it did not explain how the government would ensure that “innocent” devices or individuals were not subject to search. (Mot. at 19-21.) Mr. Epich also contends that the affidavit failed to establish that the search would uncover evidence of a crime because the search applied to all users of the website without regard to whether they violated any law. (*Id.* at 21-22.)

The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “When an affidavit is the only evidence presented to a judge in support of a search warrant, the validity of the warrant rests solely on the strength of the affidavit.” *United States v. Peck*, 317 F.3d 754, 755 (7th Cir. 2003).

“A search warrant affidavit establishes probable cause when it ‘sets forth facts sufficient to induce a reasonable prudent person to believe that a search thereof will uncover evidence of a crime.’” *United States v. Jones*, 208 F.3d 603, 608 (7th Cir. 2000) (quoting *United States v. McNeese*, 901 F.2d 585, 592 (7th Cir. 1990)). In deciding whether an affidavit establishes probable cause, “courts must use the flexible totality-of-the-circumstances standard set forth in *Illinois v. Gates*,

462 U.S. 213, 238, 103 S. Ct. 2317, 2332, 76 L. Ed. 2d 527 (1983).” *McNeese*, 901 F.2d at 592. Applying the totality-of-the-circumstances standard, “[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Gates*, 462 U.S. at 238.

“[P]robable cause is a fluid concept -- turning on the assessment of probabilities in particular factual contexts.” *Id.* at 232. Thus, “[i]n dealing with probable cause, . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.” *Brinegar v. United States*, 338 U.S. 160, 175 (1949). “Probable cause denotes more than mere suspicion, but does not require certainty.” *United States v. Anton*, 633 F.2d 1252, 1254 (7th Cir. 1980).

The court’s duty in reviewing a search warrant and its supporting materials is limited to ensuring “that the magistrate had a ‘substantial basis for . . . [concluding]’ that probable cause existed.” *Gates*, 462 U.S. at 238-39 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)). In other words,

a magistrate’s determination of probable cause is to be “given considerable weight and should be overruled only when the supporting affidavit, read as a whole in a realistic and common sense manner, does not allege specific facts and circumstances from which the magistrate could reasonably conclude that the items sought to be seized are associated with the crime and located in the place indicated.”

United States v. Pritchard, 745 F.2d 1112, 1120 (7th Cir. 1984) (quoting *United States v. Rambis*, 686 F.2d 620, 622 (7th Cir. 1982)). Even “doubtful cases should be resolved in favor of upholding the warrant.” *Rambis*, 686 F.2d at 622.

Here, Mr. Epich argues that the NIT Warrant Affidavit failed to establish probable cause to believe that every person who logged onto the website committed a crime because users could access the site without knowing its illegal nature and without violating the law. (Mot. at 19; Reply at 2; Resp. to Sur-reply at 1.) That is, according to Mr. Epich, logging onto a website that contains child pornography—in additional to other, legal material—is insufficient to establish probable cause to search every user of that site. (Mot. at 16-19 (citing *United States v. Coreas*, 419 F.3d 151 (2d Cir. 2005)).)

Upon reviewing the NIT Warrant and its supporting materials in light of the parties’ arguments and the relevant case law, the Court finds that Mr. Epich’s argument rests on a crabbed reading of the search warrant affidavit and suggests a heightened standard of probable cause not mandated by the Fourth Amendment. Accordingly, for the reasons described below, the Court is persuaded that the issuing magistrate judge had a substantial basis for concluding that, under the totality of the circumstances, there was a fair probability that evidence relating to federal violations concerning child pornography would be found by using the NIT on the target website.

A commonsense reading of the affidavit demonstrates that it is highly

unlikely that the NIT Warrant subjected to search users who stumbled upon the website by pure happenstance because users had to engage in numerous affirmative steps just to gain access to the site's content. The affidavit explained that the website operated on the anonymous Tor network, which users could access only after downloading specific Tor software. (NIT Warrant Affidavit ¶¶ 7-9.) It further explained that the website was not located on the traditional Internet and, thus, users had to know the exact web address to access the site. (*Id.* ¶ 10.) This Tor-based web address was simply "a series of algorithm-generated characters . . . followed by . . . 'onion.'" (*Id.* ¶ 9.) Thus, the web address was not something that could be easily remembered. The affidavit suggested that users could obtain the address via word of mouth or by clicking a link on a Tor "hidden service" page. (*Id.* ¶ 10.) By describing the nature of the website and the steps required to find it, the affidavit supported the reasonable inference that users likely discovered the web address via other forums dedicated to child pornography.

Moreover, although a user could accomplish the above steps with relative ease, other information contained in the affidavit bolstered the conclusion that it would be extremely unlikely that any user would access the site without understanding its purpose and content. That is, even assuming that an individual could inadvertently or innocently find the site, such users were not subject to the NIT Warrant unless he/she engaged in other activities that revealed the site's illegal nature.

After downloading the Tor software and obtaining the website's exact web

address, users arrived at the main page of the site. Straddling the site's name were "two images depicting partially clothed prepubescent females with their legs spread apart." (*Id.* ¶ 12.) While the images alone implied that the site contained illicit child pornography, this suggestion was reinforced by the text located immediately underneath the images, which read, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." (*Id.*) The affiant explained that, based on his training and experience, "no cross-board reports" referred to "a prohibition against material that is posted on other websites from being 're-posted' to [the website]," and ".7z" referred to "a preferred method of compressing large files or sets of files for distribution." (*Id.*) These technical terms thus implied that the site contained images or videos and was not simply a discussion forum or chatroom. Consequently, the juxtaposition of the suggestive images and the text referencing terms associated with sharing images and/or videos created a strong inference that the site contained child pornography.

To gain access to the site's content, users also had to register an account by accepting the site's registration terms and entering a username, password, and email address. (*Id.* ¶¶ 12-14.) The registration page further supported the inference that the site contained illicit material by advising users to provide a fake email address and by emphasizing the anonymous nature of the site. Upon registering and logging on, users gained access to all of the sections, forums, and sub-forums on the website, many of which contained images and/or videos that depicted child pornography. (*See id.* ¶¶ 14-27.) Thus, once logged on, the illegal nature of the site

was readily apparent.

To summarize, the NIT Warrant Affidavit established the following facts regarding the target website and its registered users: (1) the website operated only on an anonymous network that required users to download specific software before even finding the site; (2) finding the site required multiple, intentional steps; (3) users were unlikely to find the site without knowing its purpose and content; (4) the main page of the site depicted images that suggested the site contained child pornography and text that implied the site contained illicit images and/or videos; (5) users needed to register an account before they could access the site's content and were encouraged to use a fake email address when registering; and (6) images and videos containing child pornography were available to all users who registered an account. Based on the totality of the circumstances, these facts created a reasonable inference that registered users who accessed the website knew that it contained child pornography and accessed the site with the intent to view this illicit material. Accordingly, the issuing magistrate judge had a substantial basis for concluding that probable cause existed to issue the NIT Warrant.

That the website also contained legal material, thereby making it possible that users could visit the site without violating the law, does not alter the analysis. While courts should consider "possible innocent alternatives" in the totality-of-the-circumstances analysis, it is well-established that "the mere existence of innocent explanations does not necessarily negate probable cause."

United States v. Funches, 327 F.3d 582, 587 (7th Cir. 2003). Indeed, "probable cause

is far short of certainty—it ‘requires only a probability or substantial chance of criminal activity, not an actual showing of such activity.’” *United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012) (quoting *Gates*, 462 U.S. at 243 n.13). As described above, the totality-of-the-circumstances here established a substantial chance that registered users who accessed the website did so with the intent to view child pornography.

Similarly, the affidavit’s failure to differentiate users based on the frequency of log-ins, the duration of log-ins, or the material being accessed does not negate the probable cause finding. As other courts have accurately recognized, the probable cause analysis does not turn on what additional investigation the government *could have done*. See, e.g., *United States v. Shields*, 458 F.3d 269, 280 (3d Cir. 2006) (upholding validity of warrant authorizing search of defendant’s home even though FBI “could have” but did not “determine[] with certainty whether he actually downloaded illegal images”); *United States v. Gourde*, 440 F.3d 1065, 1072-73 & n.5 (9th Cir. 2006) (en banc) (same). The issuing judge had a substantial basis for finding probable cause even without the benefit of this additional information.

Furthermore, in contrast to Mr. Epich’s suggestion, the Second Circuit’s decision in *Coreas* does not demonstrate that probable cause was lacking in this case. In *Coreas*, a Second Circuit panel generally held that logging onto a website that contains child pornography—in addition to other, legal material—and agreeing to join its e-group does not establish probable cause to search that person’s home. *Coreas*, 419 F.3d at 156-59. A number of courts have reached the opposite

conclusion. *See, e.g., Shields*, 458 F.3d at 278-80; *Gourde*, 440 F.3d at 1069-73; *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004); *United States v. Hutto*, 84 F. App'x 6, 8 (10th Cir. 2003); *United States v. Bailey*, 272 F. Supp. 2d 822, 824-25 (D. Neb. 2003). Indeed, the *Coreas* court ultimately affirmed the defendant's conviction, finding that it was compelled by an earlier panel's decision that addressed the same issue and reached the opposite conclusion. *Coreas*, 419 F.3d at 157-59; *see United States v. Martin*, 426 F.3d 68, 74-77 (2d Cir. 2005).

Perhaps more importantly, the facts in *Coreas* are materially distinguishable from the facts at issue here. First, the court in *Coreas* implied that probable cause was lacking because there was no evidence that members knew the alleged "primary purpose" of the e-group or actually intended to take advantage of the site's illicit features. *Coreas*, 419 F.3d at 158. The court further emphasized that the search warrant affidavit did not allege that the defendant downloaded any child pornography. *Id.* at 156-57. Thus, probable cause was based solely on "clicking a button." *Id.* In this case, however, the information in the NIT Warrant Affidavit established a reasonable inference that registered users of the website knew its purpose and accessed the site with the intent to view child pornography. The users here also were subject to search only after downloading specific software, locating the website, registering an account, and logging onto the site during the two-week window the government deployed the NIT. Thus, probable cause was based on more significant conduct than simply clicking a button to join an online group.

Second, the warrant at issue in *Coreas* authorized the government "to enter

[the defendant's] private dwelling and rummage through various of his personal effects." *Coreas*, 419 F.3d at 156 (collecting cases). The NIT Warrant, in contrast, merely authorized use of the NIT to obtain information that would assist the government in identifying the website's users, namely their actual IP address. The NIT search was thus minimally invasive compared to the search authorized in *Coreas*. Of course, the information gathered from the NIT search led the government to seek warrants to search Mr. Epich's residence and a thumb drive found therein. However, the Residence Warrant and the Thumb Drive Warrant were issued only after the government conducted additional investigation that confirmed Mr. Epich had accessed from the website several posts that contained links to and sample photos of child pornography.

Mr. Epich's remaining Fourth Amendment arguments are unavailing and, therefore, require only a brief analysis. The Court finds that the NIT Warrant satisfied the Fourth Amendment's particularity requirement as it specifically described the place to be searched and the things to be seized. The search warrant affidavit outlined who would be subject to the NIT, what information the NIT would obtain from users' computers, when the NIT would be deployed; where the NIT would be deployed, why the NIT was necessary, and how the NIT would be deployed. (NIT Warrant Affidavit ¶¶ 31-37.) The affidavit also included Attachments A and B, which described, respectively, the "Place to be Searched" and the "Information to be Seized." (*See id.* at 32-33.) The affidavit further indicated that the NIT would reveal only the specific identifying information listed in

Attachment B. (*See id.* ¶ 34.) Thus, Mr. Epich’s contention that the NIT could have searched or infected innocent computers or devices, (Mot. at 20), is purely speculative and without merit.

Likewise, the information contained in the affidavit established a fair probability that deployment of the NIT would uncover evidence of a crime. In essence, the NIT would pierce the veil afforded by the anonymous Tor network and provide the government the information—i.e., the actual IP address—needed to ascertain the location and identity of the website’s users who accessed the site with the intent to view child pornography. (NIT Warrant Affidavit ¶¶ 31-37.) Put simply, such information constitutes evidence of a crime within the meaning of the Fourth Amendment.

In sum, for all the foregoing reasons, the Court finds that the NIT Warrant comported with the requirements of the Fourth Amendment.

2. The warrant’s compliance with Federal Rule Criminal Procedure 41(b)

Mr. Epich also argues that the NIT Warrant “plainly violated Rule 41 of the Federal Rules of Criminal Procedure” and that suppression is an appropriate remedy here because the violation was “prejudicial and blatant.” (*See* Mot. at 22-24; Reply at 17-22; Resp. to Sur-reply at 3-5.)

“Rule 41(b) sets out five alternative territorial limits on a magistrate judge’s authority to issue a warrant.” *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013). Specifically, Rule 41(b) authorizes magistrate judges to issue warrants to (1) search for and seize a

person or property located within the judge's district; (2) search for and seize a person or property located outside the judge's district "if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed"; (3) search for and seize a person or property located outside the judge's district if the investigation relates to terrorism; (4) "install within the district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both; or (5) search for and seize a person or property located outside the judge's district but within a United States territory, possession, commonwealth, or premises used by a United States diplomatic or consular mission. *See* Fed. R. Crim. P. 41(b).

The government argues that the NIT Warrant comported with the territorial limits set forth in Rule 41(b). (*See* Government's Response to Defendant's Motion to Suppress, ECF No. 41 at 32-35; Government's Sur-reply in Opposition to Defendant's Motion to Suppress, ECF No. 49 at 4-6.) According to the government, the NIT was essentially a set of computer instructions that the government deployed on the target website while it was running on a computer server located in the Eastern District of Virginia. When a user logged onto the website while the NIT was in effect, the user's computer downloaded the additional instructions from the server and then sent the requested information back to a server located in the Eastern District of Virginia. The government thus maintains that the NIT Warrant satisfied Rule 41(b)(1) or (b)(2) because the NIT was property located within the

district of the issuing judge and because users “reached into” the Eastern District of Virginia to access the seized website. The government also likens the NIT to a “tracking device” authorized under Rule 41(b)(4). Alternatively, the government argues that suppression is generally not an apt remedy for a Rule 41 violation and that suppression would be especially inappropriate in this case because users relied on an anonymous network to mask their identities.

Mr. Epich argues that the NIT Warrant does not fall within any of the five provisions listed in Rule 41(b). According to Mr. Epich, the NIT Warrant authorized the government to search his computer—i.e., property that was never located within the Eastern District of Virginia, let alone at the time the warrant was issued. (Reply at 17-20.) He also maintains that the identifying information sought by the warrant was not sent into the Eastern District of Virginia until users logged onto the website *after* the warrant was executed. Mr. Epich further contends that the NIT cannot be considered a tracking device because it did not track the movement of users’ computers and, in any case, the NIT was not installed within the Eastern District of Virginia.

Although Mr. Epich raises an interesting and compelling issue,¹ the Court

¹ Indeed, the Supreme Court is currently reviewing a proposed amendment to Rule 41(b) that would allow magistrate judges “to issue a warrant to use remote access to search electronic storage media” located inside or outside the judge’s district if “the district where the media or information is located has been concealed through technological means.” *See* Advisory Committee on Criminal Rules, September 2015 Agenda, at 205, available at <http://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/agenda-books>; *see also* United States Courts, Pending Rules Amendments, <http://www.uscourts.gov/rules-policies/pending-rules-amendments> (last visited Jan. 21, 2016).

need not determine whether the NIT Warrant strictly complied with the requirements of Rule 41(b) to resolve Mr. Epich's motion because suppression clearly would not be an appropriate remedy in this case. The Seventh Circuit has unequivocally held that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause, and with advance judicial approval." *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008). The court has also explicitly rejected suppression as a remedy for a Rule 41 violation, holding that "[t]he remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be 'wildly out of proportion to the wrong.'" *United States v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008) (quoting *Cazares-Olivas*, 515 F.3d at 730). Moreover, the court has expressed doubt as to whether suppression would ever be an appropriate remedy for such a violation:

In light of *Leon*, it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that would call for suppression. Many remedies may be appropriate for deliberate violations of the rules, but freedom for the offender is not among them.

United States v. Trost, 152 F.3d 715, 721-22 (7th Cir. 1998) (quoting *United States v. Hornick*, 815 F.2d 1156, 1158 (7th Cir. 1987)).

Consequently, even assuming that the NIT Warrant violated Rule 41(b), the evidence at issue here should not be suppressed because it was obtained via a judicially authorized warrant supported by probable cause. Suppression would be an especially inappropriate remedy in this case given the circumstances facing the

government. Because of the anonymizing software, the government was unable to determine the location and identity of the website's users. The NIT, however, provided the government the means to unmask these users, who were suspected of committing federal violations concerning child pornography. Likewise, the government sought the NIT Warrant in the judicial district where the seized website was located and where the NIT was to be implemented. Such conduct was reasonable under the circumstances.

Accordingly, because the NIT Warrant satisfied the requirements of the Fourth Amendment, and because suppression would be "wildly out of proportion" to any purported violation of Rule 41(b), the Court will recommend that the district judge deny Mr. Epich's motion to suppress.

NOW, THEREFORE, IT IS HEREBY RECOMMENDED that defendant Phillip A. Epich's motion to suppress, (ECF No. 34), be **DENIED**.

Your attention is directed to General L. R. 72(c) (E.D. Wis.), 28 U.S.C. § 636(b)(1)(B), and Federal Rules of Criminal Procedure 59(b) or 72(b), if applicable, whereby written objections to any recommendation herein, or part thereof, may be filed within fourteen days of the date of service of this recommendation. Objections are to be filed in accordance with the Eastern District of Wisconsin's electronic case filing procedures. Courtesy paper copies of any objections shall be sent directly to the chambers of the district judge assigned to the case. Failure to file a timely objection with the district court shall result in a waiver of a party's right to appeal. If no response or reply will be filed, please notify the Court in writing.

Dated at Milwaukee, Wisconsin, this 21st day of January, 2016.

BY THE COURT:

s/ David E. Jones
DAVID E. JONES
United States Magistrate Judge